Cybersecurity Perspectives on Technology-Facilitated Gender-Based Violence on Social Media

Abstract

Cyber harassment has become a ubiquitous and harmful kind of online bullying, which predominantly affects women. This paper investigates both the convergence of cybersecurity and gender-based violence in the online spaces. The analysis sheds light on how technological vulnerabilities are exploited in manipulation of images, blackmailing via the Internet, and identity theft by providing the scholarship of Citron (2014), Henry and Powell (2018), and empirical findings of UN Women (2024) or the European Union Agency on Cybersecurity (ENISA, 2023). The outcomes indicate that attackers use poor cybersecurity frameworks, deep-fakes, and fake identities to harass and extort victims and extort money and harass them, and governmental structures are not responsive enough to these challenges. This paper argues that cybersecurity is not merely about the protection of data, but it also involves key functions in protecting online health, cybersecurity, and gender equity in the online spaces mediated by technology.

Introduction

Online communication has spawned new possibilities of connectivity but has simultaneously created various forms of online harm. Women have been the disproportionate victims of cyber harassment, which includes non-consensual image sharing, blackmail online, and deep-fake manipulation (Citron, 2014). Citron suggests that the online hate and the use of images as a form of abuse are modern tools of digital control, the aim of which is to silence and intimidate women who speak publicly.

A 2021 study by the Pew Research center revealed that 41 percent of adults in the United States said they had been harassed online, and females were more prone to describe the experiences as very or extremely upsetting when compared to males. These findings are illustrated in figures shown below, thus picturing the gender gap and emotional consequences of online abuse.

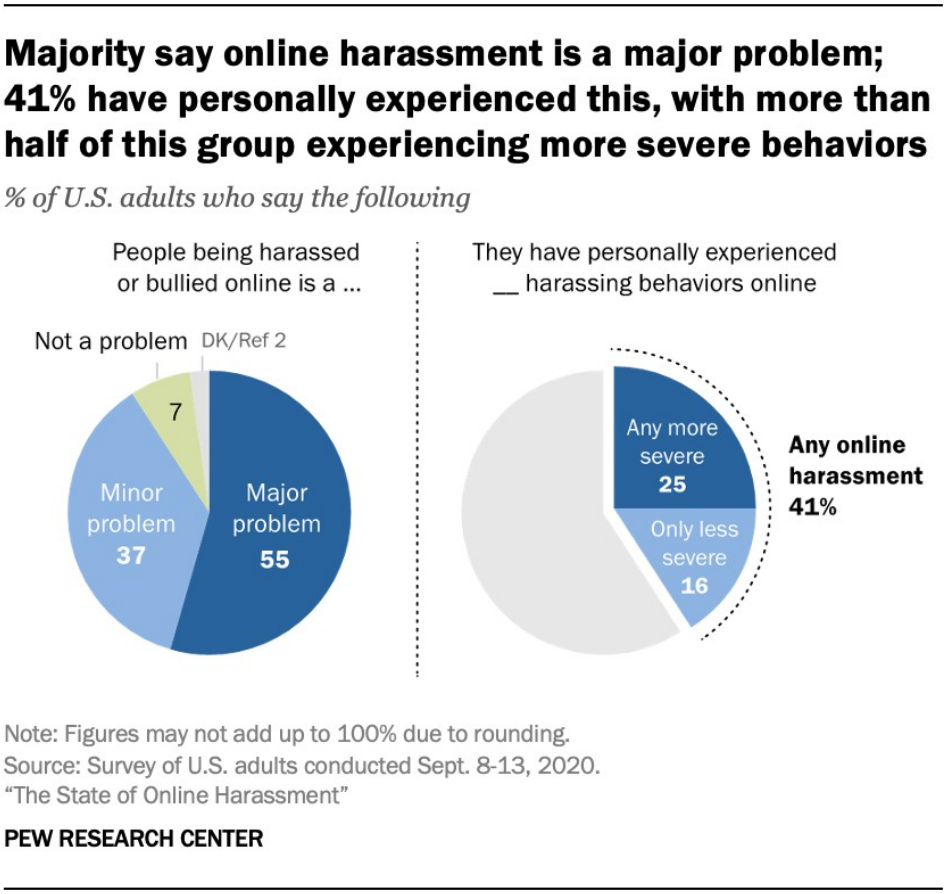
Majority say online harassment is a major problem; 41% have personally experienced this, with more than half of this group experiencing more severe behaviors
% of U.S. adults who say the following
People being harassed or bullied online is a ...
Not a problem
DK/Ref 2
7
Minor problem 37
Major problem 55
They have personally experienced __ harassing behaviors online
Any more severe 25
Only less severe 16
Any online harassment 41%
Note: Figures may not add up to 100% due to rounding.
Source: Survey of U.S. adults conducted Sept. 8-13, 2020.
"The State of Online Harassment"
PEW RESEARCH CENTER

Figure 1. Perceptions and Personal Experiences of Online Harassment Among U.S. Adults, 2020

Source: Pew Research Center, *The State of Online Harassment* (2020).

These findings suggest that cyber bullying has become a normalized social phenomenon in the electronic space. The rate of exposure of women is disproportionately higher, indicating the inefficiency of the existing moderation and reporting processes in capturing the gendered aspects of abusive behaviour. In turn, such discrepancy poses a sharp dilemma to the cybersecurity architectures that have traditionally focused on technical intrusions rather than sociocultural harms.

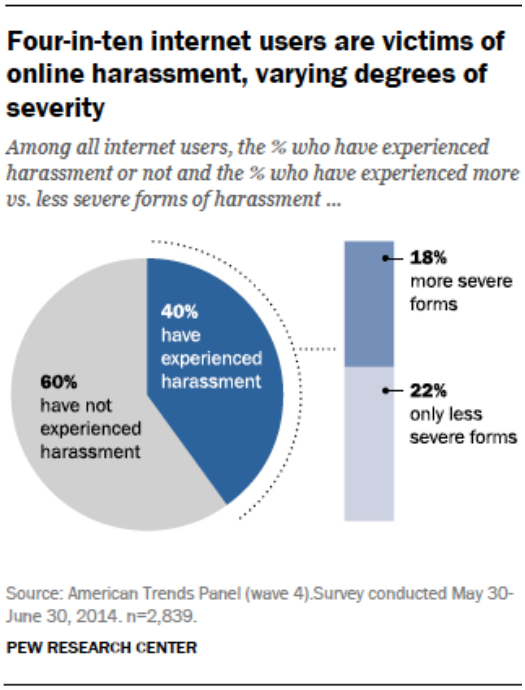
Four-in-ten internet users are victims of online harassment, varying degrees of severity
Among all internet users, the % who have experienced harassment or not and the % who have experienced more vs. less severe forms of harassment ...
40% have experienced harassment
60% have not experienced harassment
18% more severe forms
22% only less severe forms
Source: American Trends Panel (wave 4).Survey conducted May 30-June 30, 2014. n=2,839.
PEW RESEARCH CENTER

Figure 2. Prevalence and Severity of Online Harassment among Internet Users

Source: Pew Research Center (2021).

The latter visualization (Figure 2) provides a slightly different view. It does not only explain how such incidents are rampant; it also explains the resultant effect. A third of all women compared to only 14 per cent. of all men reported that they were emotionally distressed after online abuse. These data support the paradigm that the measurements of online safety should also include the number of attacks and the extent of the harm as a result of these attacks.

As the use of artificial intelligence applications and image-editing features, as well as data-tracking solutions, continues to rise, the offenders can easily exploit the loopholes in terms of security in social networks. Henry and Powell (2018) describe the described phenomena as technology-facilitated violence, highlighting the role of digital platforms as inadvertent amplifiers of gender disparities. Rather than focusing solely on individual psychological factors, this paper examines how technological infrastructures and social systems also generate vulnerability and safety risks of victims in the digital realms.

The anonymity of the internet only helps to make the problem worse. Criminals hide in encrypted networks and fake accounts, and it is hard to trace them and prosecute them (ENISA, 2023). The lack of internationally agreed-upon cybersecurity standards and international collaboration (EIGE, 2022) fosters a piecemeal implementation and a lower

level of protection to users. In terms of cybersecurity, the constant presence of image-based blackmail indicates the inadequate authentication, content control, and data management, as reported by UN Women (2023). The need to deal with these vulnerabilities requires the concerted efforts of governments, technology enterprises, and social institutions to develop safer digital ecosystems.

Methodology

This research employed a qualitative approach to literature review, analyzing academic work on cybersecurity and digital safety issued in 2015-2024. The sources will include peer-reviewed journal articles, official publications of the cybersecurity agencies, and materials of gender-equity institutions, including UN Women, ENISA, and EIGE. Based on the thematic framework developed by Henry and Powell (2018), the review aimed to identify three major themes, including (1) the abuse of technology in harassment, (2) the issue of anonymity and the impossibility of detecting deep-fakes, and (3) the constraints of the current cybersecurity regulation.

To capture generational patterns, this study incorporates Pew Research Center (2022) data on teen cyberbullying. Figure 3 and Figure 4 present visual summaries of gender differences in adolescent online harassment.

Older teen girls more likely than younger girls or boys of any age to have faced false rumor spreading, constant monitoring online, as well as cyberbullying overall

% of U.S. teens who say they have ever experienced ___ when online or on their cellphone

	Offensive name-calling	Spreading of false rumors about them	Receiving explicit images they didn't ask for	Constantly being asked where they are, what they're doing, or who they're with by someone other than a parent	Physical threats	Having explicit images of them shared without their consent	Any cyberbullying
U.S. teens	32	22	17	15	10	7	46
Boys	31	16	15	13	10	5	43
Girls	32	29	19	17	10	8	49
White	35	24	16	14	10	6	48
Black	29	17	21	9	11	10	40
Hispanic	29	21	19	21	10	7	47
Ages 13-14	29	20	11	12	10	4	42
15-17	34	24	22	17	10	8	49
Boys 13-14	31	15	11	12	10	3	41
15-17	32	16	18	13	10	7	44
Girls 13-14	25	24	10	12	9	5	41
15-17	36	33	25	20	10	9	54

Note: Teens are those ages 13 to 17. White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey conducted April 14-May 4, 2022.
"Teens and Cyberbullying 2022"

PEW RESEARCH CENTER

Figure 3. Age and Gender Differences in U.S. Teens' Experiences with Cyberbullying

Source: Pew Research Center, Teens and Cyberbullying (2022).

As it can be seen in Figure 3, cyberbullying among teenagers is represented in the same gendered trends as those recorded in the adult population. Female adolescents more frequently report having encountered some type of online harassment (more than a half) compared to male adolescents (less than half) (Pew Research Center, 2022). This age-related information suggests that the phenomenon of online aggression is rooted at a young age and continues in the adult stage.

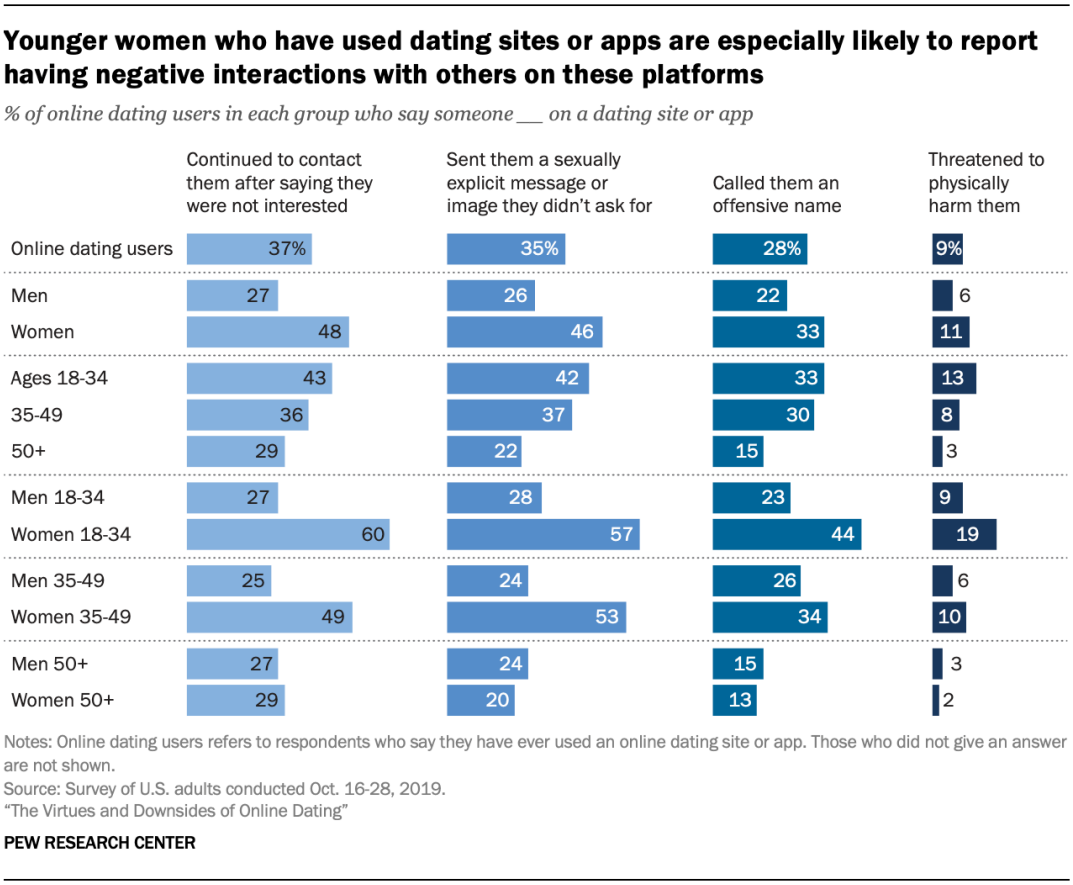
Younger women who have used dating sites or apps are especially likely to report having negative interactions with others on these platforms
% of online dating users in each group who say someone ___ on a dating site or app
Continued to contact them after saying they were not interested
Sent them a sexually explicit message or image they didn't ask for
Called them an offensive name
Threatened to physically harm them
Online dating users 37% 35% 28% 9%
Men 27 26 22 6
Women 48 46 33 11
Ages 18-34 43 42 33 13
35-49 36 37 30 8
50+ 29 22 15 3
Men 18-34 27 28 23 9
Women 18-34 60 57 44 19
Men 35-49 25 24 26 6
Women 35-49 49 53 34 10
Men 50+ 27 24 15 3
Women 50+ 29 20 13 2
Notes: Online dating users refers to respondents who say they have ever used an online dating site or app. Those who did not give an answer are not shown.
Source: Survey of U.S. adults conducted Oct. 16-28, 2019.
"The Virtues and Downsides of Online Dating"
PEW RESEARCH CENTER

Figure 4. Prevalence of Negative Interactions on Online Dating Platforms: A Demographic Analysis

Source: Pew Research Center (2021).

Lastly, Figure 4 puts the frequency of incidents by age group into perspective whereby younger groups (ages 18-29) are at the highest risk of being subjected to repeated cases of online abuse. This fact empirically supports the argument of ENISA (2023) that emerging technologies expose youth to digital threats at an accelerated rate, which cannot be adequately kept up to date by the current policy frameworks.

The reports provided by UN Women (2024) and ENISA (2023) were also reviewed to outline the trends and preventative measures at the global level. The study will focus on the technology-related factors, namely how vulnerabilities in systems and ineffective delivery of the policy contribute to the occurrence of blackmail and manipulation online. Ethical standards of research were shared through not using the explicit data of the victim and focusing on the importance of consent and privacy of data in online safety discussions.

Results

The review of the literature and the institutional reporting show that gender-based cyber harassment is often the antecedent of serious social and digital safety issues. Victims face such threats as reputational harm, loss of online presence, and identity theft (Henry & Powell, 2018; UN Women, 2023). The European Institute of Gender Equality (2022) claimed that 1 out of every 4 women in the European Union has faced some kind of online abuse, and in most of the cases, no one reports it because the system does not provide trust in the resources of the law or digital protection.

Citron (2014) claims that the problem of online abuse is often underestimated by law-enforcement agencies that do not understand its seriousness as per the current cybersecurity policies. Technically, ENISA (2023) highlights the lack of algorithmic content detection and cross-border cybercrime collaboration. The implication of these findings is that infrastructural security measures are not sufficient to address modern cybersecurity mechanisms; simultaneous work should be carried out on anticipating possible threats on the Internet, implementing AI-based content filtering, and investing in digital literacy in society. Solid security protocols could also become crucial in ensuring that gender equality occurs online and also by minimizing the percentage of harassment and also by improving accountability in the technology industry.

Conclusion

Gender-based violence that is facilitated by technology can be used to understand how cybersecurity problems intersect with social justice. Although online protection is based on encryption, AI moderation tools, and authentication systems, they cannot be considered a replacement to extensive education, awareness, and legislative measures (ENISA, 2023). According to the UN Women (2024), to address the issue of digital abuse, the integration of cybersecurity systems with the gender-sensitive and diversity-friendly technology design and formation of ethical policies are necessary.

This paper finds out that digital safety is not a purely technical issue; it is a wider human rights challenge that entails privacy, equality and responsibility in the virtual world. Governments, developers, and the internet platforms should increase the level of exposure of content moderation, employ more robust user authentication protocols, and initiate collaboration between cybersecurity specialists and feminists. The next generation of studies should be on designing ethical AI tools that would identify harmful trends while maintaining privacy. The most effective way to make the digital environments safe and

more equal to everyone is the creation of a holistic approach to cybersecurity that would co-locate both technical innovation and social awareness.

0”„„„„„„„„„„„„„„„„„„/

References

- Amnesty International. (2018). *#ToxicTwitter: Violence and abuse against women online.* https://www.amnesty.org/en/documents/act30/8070/2018/en/
- Citron, D. K. (2014). *Hate Crimes in Cyberspace.* Harvard University Press.
- Citron, D. K. (2015). An overview of hate crimes in cyberspace. *Case Western Reserve Journal of Law, Technology & the Internet, 6*(1). https://scholarlycommons.law.case.edu/jolti/vol6/iss1/3/
- European Institute for Gender Equality (EIGE). (2022). *Combating cyber violence against women and girls.* https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf
- European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- Henry, N., & Powell, A. (2018). *Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19*(2), 195–208. https://doi.org/10.1177/1524838016650189
- Pew Research Center. (2021). *The State of Online Harassment.* https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/
- Pew Research Center. (2022). *Teens and Cyberbullying.* https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/
- UN Women. (2024). *Technology-facilitated violence against women and girls – Report of the UN Secretary-General (A/79/500).* https://www.unwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024.pdf